U.S. NAVAL ACADEMY
COMPUTER SCIENCE DEPARTMENT
TECHNICAL REPORT

On Quantifer Elimination by Virtual Term Substitution

Brown, Christopher W.

USNA-CS-TR-2005-07

August 24, 2005

USNA Computer Science Dept. ◦ 572M Holloway Rd Stop 9F ◦ Annapolis, MD 21403

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
24 AUG 2005		**00-08-2005 to 00-08-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
On Quantifer Elimination by Virtual Term Substitution	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Naval Academy,Computer Science Department,572M Holloway Rd Stop 9F,Annapolis,MD,21403**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**19**	

On Quantifier Elimination by Virtual Term Substitution

Christopher W. Brown
Computer Science Department, Stop 9F
United States Naval Academy
572M Holloway Road
Annapolis, MD 21402
wcbrown@usna.edu

August 4, 2005

Abstract

This paper presents a new look at Weispfenning's method of quantifier elimination by virtual term substitution and provides two important improvements. Virtual term substitution eliminates a quantified variable by substituting formulas in the remaining variables for each atomic formula in which the quantified variable appears. This paper investigates the polynomials that arise in substitution formulas Weispfenning proposed and, based on this examination, provides a simpler substitution for the general case, and alternate substitutions for several commonly occurring situtions. Providing alternate substitutions allows virtual term substitution to make choices that produce simpler output.

1 Introduction

Quantifier elimination for elementary real algebra is a fundamental problem in symbolic computing. The great potential utility of quantifier elimination algorithms is, however, offset by an equally great theoretical and practical complexity. Thus, the search for improved algorithms that are capable of solving interesting problems in a reasonable amount of time and space is important.

One successful result of this ongoing search is Weispfenning's method of quantifier elimination by virtual term substitution [4, 6, 5]. This method, restricted to formulas that are linear or quadratic in the quantified variable, has been

implemented in the Redlog system [2], and has been applied successfully to a number of practical problems (e.g. [7]).

The strength of quantifier elimination by virtual term substitution is that its complexity is relatively unaffected by the number of parameters — i.e. unquantified variables — in the problem. The method has two weaknesses: First, applying the method iteratively to eliminate several quantified variables may not be possible because eliminating one variable may increase the degrees of remaining variables, thus violating the degree restrictions. Second, quantifier-free equivalent formulas produced by the method tend to be very large, even when simple quantifier-free equivalents exist.

The purpose of this paper is to provide a new perspective on virtual term substitution, and to apply this new perspective to help address the method's weaknesses.

1.1 What's new

Virtual term substitution is based on rewriting. A formula $\exists x[F]$ is transformed into an equivalent formula in which x does not appear by combining many copies of F in which atomic formulas are substituted by more complex formulas. In this paper we give a new analysis of which polynomials appear in these substitution formulas and why. Using this analysis, we provide an improved substitution (Section 3) for the algorithm's general case: improved in that fewer atomic formula and fewer distinct polynomials appear in the output formula. Generically, the improved method produces a formula in which the set of polynomials occurring is a proper subset of those occurring in the original method's output.

Also using our initial analysis, we provide alternate substitutions which may be used in certain situations — allowing the method to evaluate alternatives and choose the best substitution (see Section 4). In particular, substitutions which use lower degree polynomials or which allow obvious simplifications can be chosen.

Two detailed examples applying both improvements are given in Section 5. The ideas presented here have not yet been implemented, so experimental data on a wide range of benchmark problems cannot be given.

Finally, Section 6 applies the characterization from previous sections of the polynomials appearing in substitutions to determine a new bound on the degree of any irreducible factor of a polynomial appearing in the formula resulting from eliminating a variable.

2 Evaluating a formula at a quadratic's roots

Suppose we want to eliminate x from the formula $\exists x[f = 0 \wedge F]$, where $f = ax^2 + bx + c$ and each atomic formula in F is of the form $g\ \sigma\ 0$. Theorem 2.1 of [6] describes the *virtual term substitution* approach to solving this problem. Virtual term substitution starts by substituting $(-b \pm \sqrt{D})/2a$ for x in F. Each atomic formula $g((-b \pm \sqrt{D})/2a)\ \sigma\ 0$ is then replaced by an equivalent formula without radicals.

For the rest of this section we let $f = ax^2 + bx + c$, $D = b^2 - 4ac$, $\alpha_{+1} = (-b + \sqrt{D})/2a$, $\alpha_{-1} = (-b - \sqrt{D})/2a$, and let g be an integral polynomial of positive degree n in x. First we will prove some simple results concerning $g(\alpha_{\pm 1})$. Then we will restate the substitution described in Theorem 2.1 of [6].

2.1 Evaluating g at the roots of f

The following results provide several characterizations of the evaluation of a polynomial at a root of a quadratic. They are the basis of this paper's discussion of virtual term substitution.

Lemma 1 *For $k \geq 1$, $(-b + \sqrt{b^2 - 4ac})^k = 2^{k-1}\left(U_k + V_k\sqrt{b^2 - 4ac}\right)$, where U_k and V_k are integral homogeneous polynomials of total degree k and $k-1$ respectively, such that $U_k - bV_k$ has even integer content.*

Proof. We proceed by induction on k. The lemma clearly holds for $k = 1$ since $U_1 = -b$, $V_1 = 1$, and $U_1 - bV_1 = -2b$. Suppose the lemma holds for some k. Then

$$\begin{aligned}(-b + \sqrt{b^2 - 4ac})^{k+1} &= 2^{k-1}(U_k + V_k\sqrt{b^2 - 4ac})(-b + \sqrt{b^2 - 4ac}) \\ &= 2^{k-1}\left((-b(U_k - bV_k) - 4acV_k) + (U_k - bV_k)\sqrt{b^2 - 4ac}\right)\end{aligned}$$

By supposition, $U_k - bV_k = 2A$ for some integral polynomial A of total degree k, which clearly must be homogeneous. Therefore,

$$-b(U_k - bV_k) - 4acV_k = -b(2A) - 4acV_k = 2(-bA - 4acV_k)$$

which has total degree $k+1$ and is also clearly homogeneous. So $(-b + \sqrt{b^2 - 4ac})^{k+1} = 2^k U_{k+1} + 2^k V_{k+1}\sqrt{b^2 - 4ac}$, where $U_{k+1} = -bA - 4acV_k$ and $V_{k+1} = A$. Finally, we note that

$$U_{k+1} - bV_{k+1} = -bA - 4acV_k - bA = -2bA - 4acV_k$$

which clearly has even integer content. □

Theorem 1 *Formal substitution of $x = \alpha_p$ into $g(x)$ yields $(a^* + pb^*\sqrt{D})/(2a^n)$, where a^* and b^* are integral polynomials.*

Theorem 2 *Let a^* and b^* be as above and let $\delta = n \bmod 2$. $\mathrm{res}_x(f,g) = (a^{*2} - b^{*2}D)/(4a^n)$ and $\mathrm{sgn}(g(\alpha_{+1})g(\alpha_{-1})) = \mathrm{sgn}(a^{*2} - b^{*2}D) = \mathrm{sgn}(a^{\delta}\mathrm{res}_x(f,g))$.*

PROOF. By a well-known theorem (see for example [1]) $\mathrm{res}_x(f,g) = a^n \Pi_{i=1}^m g(\alpha_i)$, where $m = deg_x(f)$, $n = deg_x(g)$ and the roots of f are $\alpha_1, \ldots, \alpha_m$. So:

$$\begin{aligned} \mathrm{res}_x(f,g) &= a^n g(\tfrac{-b+\sqrt{D}}{2a}) g(\tfrac{-b-\sqrt{D}}{2a}) \\ &= a^n \left(\tfrac{a^* + b^*\sqrt{D}}{2a^n}\right)\left(\tfrac{a^* - b^*\sqrt{D}}{2a^n}\right) \\ &= (a^{*2} - b^{*2}D)/(4a^n) \end{aligned}$$

The rest follows easily. □

Theorem 3 *Let $\mathrm{prem}(g,f) = rx + s$. Then*

1. *$b^* = r = psc_1(g,f)$,*
2. *$a^* = 2as - br = -rf_x(-s/r)$, and*
3. *$4a^n\mathrm{res}_x(f,g) = 4a(as^2 - srb + r^2c) = a^{*2} - b^{*2}D$.*

PROOF. Since $\mathrm{prem}(g,f) = rx + s$, we have $a^{n-1}g = Qf + rx + s$, where Q is a polynomial. So

$$\begin{aligned} a^{n-1}g(\tfrac{-b+\sqrt{D}}{2a}) &= Q(\tfrac{-b+\sqrt{D}}{2a}) f(\tfrac{-b+\sqrt{D}}{2a}) + r(\tfrac{-b+\sqrt{D}}{2a}) + s \\ a^{n-1}g(\tfrac{-b+\sqrt{D}}{2a}) &= r(\tfrac{-b+\sqrt{D}}{2a}) + s \\ g(\tfrac{-b+\sqrt{D}}{2a}) &= \tfrac{2as - rb + r\sqrt{D}}{2a^n} \end{aligned}$$

Since $\mathrm{prem}(g,f) = \mathrm{sres}_1(g,f)$, $r = \mathrm{psc}_1(g,f)$. That $2as - br = -\mathrm{res}_x(rx + s, f_x) = -rf_x(-s/r)$ and $4a^n\mathrm{res}_x(f,g) = a^{*2} - b^{*2}D = 4a(as^2 - srb + r^2c)$ are easily checked by simple calculations. □

2.2 Virtual term substitution with a quadratic constraint

We are now ready to restate the substitutions from Theorem 2.1 of [6], which eliminate x from a formula of the form $\exists x[f = 0 \wedge F]$.

Theorem 4 *(Weispfenning) Let $f = ax^2 + bx + c$ and let g be an integral polynomial of degree n in x. Let $\delta = n \bmod 2$ and let $R = 4a(as^2 - srb + r^2c)$. Assuming $a \neq 0 \wedge b^2 - 4ac \geq 0$,*

1. $g(\alpha_p) = 0 \Longleftrightarrow pra^* \leq 0 \wedge R = 0$.
2. $g(\alpha_p) \neq 0 \Longleftrightarrow pra^* > 0 \vee R \neq 0$.
3. $g(\alpha_p) < 0 \Longleftrightarrow a^*a^\delta < 0 \wedge R > 0 \vee pra^\delta \leq 0 \wedge (a^*a^\delta < 0 \vee R < 0)$
4. $g(\alpha_p) \leq 0 \Longleftrightarrow a^*a^\delta \leq 0 \wedge R \geq 0 \vee pra^\delta \leq 0 \wedge R \leq 0$

Corollary 1 *Given the assumptions above,*

$$g(\alpha_p) < 0 \Longleftrightarrow a^*a^\delta < 0 \wedge R > 0 \vee pra^\delta < 0 \wedge (a^*a^\delta < 0 \vee R < 0).$$

Proof. Note that 3) from above can be written equivalently as $a^*a^\delta < 0 \wedge R > 0 \vee pra^\delta < 0 \wedge (a^*a^\delta < 0 \wedge R = 0 \vee R < 0)$. Recall that $R = a^{*2} - r^2D$, so $R < 0 \Longrightarrow r \neq 0$ and $R = 0 \wedge r = 0 \Longrightarrow a^* = 0$. So, $pra^\delta = 0$ is inconsistent with both $a^*a^\delta < 0 \wedge R = 0$ and $R < 0$. □

There is some reason to consider this alternative substitution for $g < 0$, since a simplifier that removes inconsistent subformulas might more easily recognise an unsatisfiable branch with $pra^\delta < 0$ rather than $pra^\delta \leq 0$ — if r was a sum of squares, for instance.

Let F_{α_p} be the formula obtained by replacing each atomic formula $g\ \sigma\ 0$ with the appropriate formula from Theorem 4. Let $F_{-c/b}$ be the formula obtained by replacing atomic formula $g\ \sigma\ 0$ with $res(bx + c, g)$, noting that if $b \neq 0$, $res(bx + c, g) = b^2g(-c/b)$.

Theorem 5 *(Weispfenning) Under the assumption $a \neq 0 \vee b \neq 0 \vee c \neq 0$*

$$\exists x[f = 0 \wedge F] \Longleftrightarrow a = 0 \wedge b \neq 0 \wedge F_{-c/b} \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge (F_{\alpha_{-1}} \vee F_{\alpha_{+1}}).$$

This gives us quantifier elimination for formulas of the form $\exists x[f = 0 \wedge F]$ under the assumption that a, b and c do not vanish simultaneously.

3 Evaluating a formula near a quadratic's roots

Theorem 3.1 of [6] gives a method for eliminating x from a formula $\exists xF$ that does not necessarily have an equational constraint, provided that all irreducible

factors of polynomials in F (recall that atomic formulas are normalized to $g\ \sigma\ 0$) have degree at most two. The approach is based on introducing the positive infinitesimal ϵ in the substituted expressions and formal substitution of $-\infty$.

The idea is as follows, there is an x satisfying F if and only if F is satisfied at $x = \alpha$ or $x = \alpha + \epsilon$ for some real root α of a polynomial in F, or at $x = -\infty$. This is clear because the truth value of F can only change as x passes through a root of the left-hand side of some atomic formula. Thus, $\exists x[F]$ is equivalent to the disjunction of F evaluated at each of these candidate points. Weispfenning improves on this by showing that if a polynomial f only appears in the atomic formulas $f = 0$ or $f \leq 0$, the point $x = \alpha + \epsilon$ where $f(\alpha) = 0$ does not need to be tested. Similarly, if f only appears in the atomic formulas $f < 0$ or $f \neq 0$, the point $x = \alpha$ does not need to be tested.

In this section we restate Weispfenning's original virtual term substitution method, then provide a different substitution for infinitesimal expressions, one that uses fewer atomic formulas and, more importantly, fewer distinct polynomials. In particular, the polynomials in the resulting formula are the same regardless of whether or not substitution of infinitesimals is required.

3.1 Virtual term substitution for formulas with x-degree at most 2

Evaluating F at a point α, where α is the root of the left-hand side of some atomic formula, has already been addressed. Evaluating F at $-\infty$ is straightforward. Therefore, evaluating F at $\alpha + \epsilon$, where α is the root of the left-hand side of some atomic formula, is what remains. Weispfenning accomplishes this by considering the derivatives of polynomials appearing in F, and thus reduces the determination of the sign of a polynomial g at $\alpha + \epsilon$ to the determination of the sign of g and its derivatives at α. In short, the infinitesimals are removed, but at the cost of introducing new polynomials.

Theorem 6 *(Weispfenning) Let $f = ax^2 + bx + c$ and let $g = a_g x^2 + b_g x + c_g$. Assuming $a \neq 0 \wedge b^2 - 4ac \leq 0$,*

1. $g(\alpha_p + \epsilon) = 0 \iff a_g = 0 \wedge b_g = 0 \wedge c_g = 0$
2. $g(\alpha_p + \epsilon) \neq 0 \iff a_g = 0 \vee b_g = 0 \vee c_g = 0$
3. $g(\alpha_p + \epsilon) < 0 \iff g(\alpha_p) < 0 \vee g(\alpha_p) = 0 \wedge (g_x(\alpha_p) < 0 \vee g_x(\alpha_p) = 0 \wedge a_g < 0)$
4. $g(\alpha_p + \epsilon) \leq 0 \iff g(\alpha_p + \epsilon) = 0 \vee g(\alpha_p + \epsilon) < 0.$

Assuming $a = 0 \wedge b \neq 0$, all of the above holds simply replacing α_p with $-c/b$.

Let $F_{\alpha_p+\epsilon}$ denote the formula obtained by carrying out the $a \neq 0$ substitutions for each element of F. Let $F_{-c/b+\epsilon}$ denote the formula obtained by carrying out the $a = 0$ substitutions for each element of F. Let $F_{-\infty}$ denote the formula obtained by replacing $g = 0$ with $\bigwedge_{i=0}^{n} g_i = 0$, $g \neq 0$ with $\bigvee_{i=0}^{n} g_i \neq 0$, and $g < 0$ with $\bigvee_{i=0}^{n} \left((-1)^i g_i < 0 \wedge \bigwedge_{j=i+1}^{n} g_j = 0\right)$, where $g = g_n x^n + \cdots + g_0$.

Let $f_i = a_i x^2 + b_i x + c_i$ be the polynomial occurring in the ith atomic formula, $f_i \ \sigma_i \ 0$. Let $D_i = b_i^2 - 4a_i c_i$ and let $\alpha_{i,\pm 1} = (-b_i \pm \sqrt{b_i^2 - 4a_i c_i})/(2a_i)$. Let I and J be the sets of indices i such that σ_i is $=, \leq$ and $<, \neq$, respectively.

Theorem 7 *(Weispfenning)* $\exists x[F]$ *is equivalent to*

$$\begin{array}{l}
\bigvee_{i \in I} \left(a_i = 0 \wedge b_i \neq 0 \wedge F_{-c_i/b_i} \vee a_i \neq 0 \wedge D_i \geq 0 \wedge (F_{\alpha_{i,+1}} \vee F_{\alpha_{i,-1}})\right) \\
\vee \\
\bigvee_{i \in J} \left(a_i = 0 \wedge b_i \neq 0 \wedge F_{-c_i/b_i+\epsilon} \vee a_i \neq 0 \wedge D_i \geq 0 \wedge (F_{\alpha_{i,+1}+\epsilon} \vee F_{\alpha_{i,-1}+\epsilon})\right) \\
\vee \\
F_{-\infty}
\end{array}$$

Notice that if there are no strict inequalities there is no need to evaluate at a point defined by infinitesimals. Evaluation at infinitesimals can be undesirable because substitutions for $g(\alpha_p + \epsilon) < 0$ and $g(\alpha_p + \epsilon) \leq 0$ require substitutions for $g_x(\alpha_p + \epsilon) < 0$, which means more atomic formulas in the substituted expressions, and more distinct polynomials. That the expression substituted for $g_x(\alpha_p + \epsilon) < 0$ really contains additional polynomials can be checked by simple calculation.

- If $f = ax^2 + bx + c$ and $g = ux^2 + vx + w$, then $r = av - ub$, $a^* = 2a^2w - 2auc - bav + ub^2$, and $R = 4a(u^2c^2 - 2ucaw + a^2w^2 - vubc - vbaw + av^2c + wub^2)$.
- If $f = ux^2 + vx + w$ and $g = ax^2 + bx + c$, then $r = -(av - ub)$, $a^* = 2u^2c - 2uaw - vub + av^2$, and $R = 4u(u^2c^2 - 2ucaw + a^2w^2 - vubc - vbaw + av^2c + wub^2)$.
- If $f = ax^2 + bx + c$ and $g = 2ux + v$, then $r = 2u$, $a^* = 2(av - ub)$, and $R = 4a(4u^2c - 2vub + av^2)$

This shows clearly that the substitution for $g(\alpha_p + \epsilon) < 0$ contains the polynomial $4u^2c - 2vub + av^2$ which is a part of neither the substitutions for $g(\alpha_p)\sigma 0$ nor $f(\beta_p)\sigma 0$, where β_p is a root of g. Thus, generically, the quantifier-free formula produced by Theorem 7 contains more atomic formulas and more distinct polynomials when infinitesimals are required than when they are not.

3.2 A simpler substitution for infinitesimals

In this section we give a simpler substitution for infinitesimals — one that uses fewer atomic formulas but which, more importantly, uses the same polynomials as are used without infinitesimals. The key observation (see Theorem 3) is that $a^* = -rf_x(-s/r)$, so that if $R = 0 \neq r$, the signs of a^* and r give the sign of f_x at the common root of f and g.

Let f, r, s and a^* be as before, but let $g = a_g x^2 + b_g x + c_g$. Let $\text{prem}(f, g) = r_g x + s_g$, and note that $r_g = -r$ and $s_g = -s$, since $\text{prem}(f, g) = -\text{prem}(g, f)$. Let $b_g^* = r_g = -r$ and let $a_g^* = 2a_g s_g - b_g r_g = -r_g g_x(-s_g/r_g) = rg_x(-s/r)$.

Theorem 8 *$g(\alpha_p + \epsilon) < 0$ is equivalent to*

$$\begin{array}{c} R > 0 \wedge a^* a^\delta < 0 \vee pra^\delta < 0 \wedge (a^* a^\delta < 0 \vee R < 0) \\ \vee \\ R = 0 \wedge \big(r = 0 \wedge pa_g < 0 \vee a^* pr \leq 0 \wedge ra_g^* < 0 \vee a^* pr < 0 \wedge a_g^* = 0 \wedge a_g < 0\big) \end{array}$$

under the assumption $a \neq 0 \wedge b^2 - 4ac \geq 0$ for $p = +1$ and $a \neq 0 \wedge b^2 - 4ac > 0$ for $p = -1$.

Proof. $g(\alpha_p + \epsilon) < 0$ is equivalent to $g(\alpha_p) < 0 \vee g(\alpha_p) = 0 \wedge (g_x(\alpha_p) < 0 \vee g_x(\alpha_p) = 0 \wedge a_g < 0)$. The first line of the substitution formula from the theorem statement is equivalent to $g(\alpha_p) < 0$ by Theorem 4 and Corollary 1, so we focus on the $g(\alpha_p) = 0$ case.

$g(\alpha_p) = 0$ is equivalent to $a^* pr \leq 0 \wedge R = 0$. If $R = r = 0$, f and g have the same roots. In this case, $g(\alpha_p + \epsilon) < 0$ if and only if the roots are distinct and the sign a_g is opposite of p, or α_p is a double root, in which case the sign of a_g must be negative: i.e. $b^2 - 4ac > 0 \wedge pa_g < 0 \vee b^2 - 4ac = 0 \wedge a_g < 0$. If $p = +1$ or $b^2 - 4ac > 0$ this can be simplified to $pa_g < 0$.

If $R = 0 \neq r \wedge a^* pr \leq 0$ then f and g have the single common root $\alpha_p = -s/r$. In this case, $a_g^* = rg_x(-s/r) = rg_x(\alpha_p)$. Therefore, $rg_x(\alpha_p) < 0 \Rightarrow g(\alpha_p + \epsilon) < 0$ and $rg_x(\alpha_p) > 0 \Rightarrow g(\alpha_p + \epsilon) > 0$. If $rg_x(\alpha_p) = 0$, α_p is a double root of g and a simple root of f, so $g(\alpha_p + \epsilon) < 0 \iff a_g < 0$.

So, $g(\alpha_p) = 0 \wedge g(\alpha_p + \epsilon) < 0$ is equivalent to

$$\begin{array}{l} R = 0 \wedge r = 0 \wedge pa_g < 0 \ \vee \ R = 0 \wedge a^* pr \leq 0 \wedge ra_g^* < 0 \vee \\ R = 0 \wedge a^* pr \leq 0 \wedge r \neq 0 \wedge a_g^* = 0 \wedge a_g < 0 \end{array} \tag{1}$$

assuming $a \neq 0 \wedge b^2 - 4ac \geq 0$ when $p = +1$ and $a \neq 0 \wedge b^2 - 4ac > 0$ when $p = -1$.

If $R = 0 \neq r$, $a^* = a_g^* = 0$ implies $f_x(-s/r) = g_x(-s/r) = 0$. But this means f and g share a double root, which contradicts $r \neq 0$. Thus, $R = 0 \wedge a^* pr \leq 0 \wedge r \neq 0 \wedge a_g^* = 0 \wedge a_g < 0$ is false when $a^* = 0$, and we may simplify it to $R = 0 \wedge a^* pr < 0 \wedge a_g^* = 0 \wedge a_g < 0$. So (1) simplifies to

$$R = 0 \wedge \left(r = 0 \wedge pa_g < 0 \vee a^* pr \leq 0 \wedge ra_g^* < 0 \vee a^* pr < 0 \wedge a_g^* = 0 \wedge a_g < 0\right).$$

□

The previous theorem showed that when both f and g have degree two $g(\alpha_p + \epsilon)\ \sigma\ 0$ and $f(\beta_q + \epsilon)\ \rho\ 0$ can be rewritten without radicals or infinitesimals using the same polynomials that are used in rewriting $g(\alpha_p)\ \sigma\ 0$ and $f(\beta_q)\ \rho\ 0$ without radicals. The next theorem shows the same thing when f has degree two and g has degree one.

Theorem 9 *If $g = ux + v$, where $u \neq 0$, and let $\beta = -v/u$, so that $f(\beta) = 0$. Let $\overline{R} = R/(4a)$, noting that the division is exact.*

$$f(\beta + \epsilon) < 0 \Longleftrightarrow \overline{R} < 0 \vee \overline{R} = 0 \wedge (-ua^* < 0 \vee a^* = 0 \wedge a < 0).$$

Note that we do not assume that $a \neq 0$.

Proof. First note that $R/(4a) = \mathrm{res}_x(f, g) = \mathrm{res}_x(g, f) = u^2 f(\beta)$, so that the sign of $\overline{R}$ is the sign of $f(\beta)$. Then note that $\mathrm{prem}(g, f) = g = ux + v$, so $r = u$ and $s = v$. Thus, by Theorem 3, $a^* = -rf_x(-s/r) = -uf_x(\beta)$. Since $u \neq 0$, $\mathrm{sgn}(f_x(\beta)) = \mathrm{sgn}(-ua^*)$. So, $f(\beta + \epsilon) < 0$ is equivalent to

$$\underbrace{\overline{R} < 0}_{f(\beta)<0} \vee \underbrace{\overline{R} = 0 \wedge -ua^* < 0}_{f(\beta)=0 \wedge f_x(\beta)<0} \vee \underbrace{\overline{R} = 0 \wedge a^* = 0 \wedge a < 0}_{f(\beta)=f_x(\beta)=0 \wedge a<0}.$$

□

The important thing about this theorem is that it shows that rewriting $f(\beta+\epsilon) < 0$ (or ≤ 0) does not require any polynomials that are not already required in rewriting $g(\alpha_p)\ \sigma\ 0$. Notice that $g(\alpha_p + \epsilon)$ can be rewritten by specializing Theorem 8 setting $a_g = 0$, $b_g = u$, $c_g = v$.

Finally, note that substitution in the case where both f and g are linear is straightforward. If $f = ax + b$, $\alpha = -b/a$, and $g - ux + v$, then $g(\alpha)\ \sigma\ 0$ is equivalent to $a\ \mathrm{res}_x(f, g)\ \sigma\ 0$, and $g(\alpha+\epsilon) < 0$ is equivalent to $g(\alpha) < 0 \vee g(\alpha) = 0 \wedge u < 0$. Thus, for any combination of degrees of f and g we have substitutions for roots, possibly with infinitesimals, that involve at most the coefficients of f and g, discriminants, pairwise resultants, first principal subresultant coefficients, and a^* and a_g^*. Using the substitutions from Theorem's 8 and 9, we must use the following slight modification of Theorem 7:

Theorem 10 *$\exists x[F]$ is equivalent to*

$$\begin{array}{l}
\bigvee_{i\in I}\left(a_i = 0 \wedge b_i \neq 0 \wedge F_{-c_i/b_i} \vee a_i \neq 0 \wedge D_i \geq 0 \wedge (F_{\alpha_{i,+1}} \vee F_{\alpha_{i,-1}})\right) \\
\vee \\
\bigvee_{i\in J}\left(a_i = 0 \wedge b_i \neq 0 \wedge F_{-c_i/b_i+\epsilon} \vee a_i \neq 0 \wedge \left(\begin{array}{c} D_i \geq 0 \wedge F_{\alpha_{i,+1}+\epsilon} \\ \vee \\ D_i > 0 \wedge F_{\alpha_{i,-1}+\epsilon} \end{array}\right)\right) \\
\vee \\
F_{-\infty}
\end{array}$$

The difference between Theorem 10 and Theorem 7 is that instead of assuming $D_i \geq 0$ for both $F_{\alpha_{i,+1}+\epsilon}$ and $F_{\alpha_{i,-1}+\epsilon}$, we assume $D_i \geq 0$ for $F_{\alpha_{i,+1}+\epsilon}$, and assume $D_i > 0$ for $F_{\alpha_{i,-1}+\epsilon}$. We do this, of course, to meet the requirements of Theorem 8. However, it makes a certain sense, because now the $D_i = 0$ case is covered by just one subformula. Another tangible benefit of this comes from the nice way we can substitute for $f(\alpha_p + \epsilon) < 0$, i.e. f evaluated to the right of one of its own roots. This can now be rewritten as $a < 0$ when $p = +1$ and $a > 0$ for $p = -1$, because the possibility of a double-root when $p = -1$ has been eliminated.

4 A different view of virtual term substitution

The fundamental question to be addressed in the quadratic case of virtual substitution is this: What is the sign of g at root α_p of $f = ax^2+bx+c$? (Assuming, of course, that $a \neq 0$ and $b^2 - 4ac \geq 0$.) The answer to this question has to be expressed as a combination of polynomial equalities and inequalities in the remaining variables — i.e. without x. In this section we give a geometric view of how this is done and, based on that view, suggest alternatives to the substitutions given in Theorem 4.

4.1 A geometric view of evaluation at roots of f

Recall that $R = 4a^n \mathrm{res}_x(f, g)$, so that R has the same sign as the product of g evaluated at the two roots of f. There is a geometry to this problem of determining the sign of g at α_p that can be seen quite clearly by considering r and s in $R = 4a(as^2 - srb + r^2c)$ as variables and a, b, and c as constant. R is the product of two lines through the origin:

$$R \quad = \quad 4a^2\left(\tfrac{-b+\sqrt{b^2-4ac}}{2a}r + s\right)\left(\tfrac{-b-\sqrt{b^2-4ac}}{2a}r + s\right)$$

For a specific g: If (r, s) falls on the first line $g(\alpha_+) = 0$. If (r, s) falls below the first line $g(\alpha_+) < 0$. If (r, s) falls on the second line $g(\alpha_-) = 0$. If (r, s) falls

below the second line, $g(\alpha_-) < 0$. In other words, the sign of $g(\alpha_p)$ is determined by where (r, s) falls with respect to these two lines. Figure 4.1 illustrates this for a specific f.

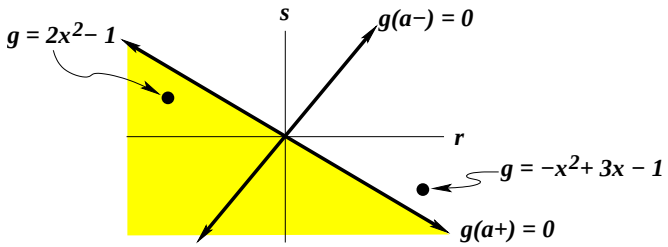

Figure 1: The region in which $g(\alpha_+) < 0$, for $f = x^2 + x - 1$. Points in the (r, s)-plane corresponding to two different g's are shown.

Of course we do not want to evaluate $\frac{-b+\sqrt{b^2-4ac}}{2a}r + s$ and $\frac{-b-\sqrt{b^2-4ac}}{2a}r + s$ directly, because they involve radicals. Instead we evaluate R, a multiple of their product. However, there are 9 possible combinations of sign for the two linear factors, and only 3 possible signs for R. Thus, other polynomials need to be introduced to distinguish between regions in which the sign of R is the same, but the signs of the linear factors are different. This is precisely the role of r and a^*.

Since $r = 0 \implies R > 0$, r always separates the two regions in which $R < 0$. Since $4a^2$, the leading coefficient of R as a polynomial in s, is always positive, $\partial R/\partial s = 4a(2as - rb) = 4aa^*$ always separates the two regions in which $R > 0$. Geometrically, r and a^* do nothing more than distinguish between disconnected regions in which R has the same sign. (Except at the origin, where they partition $R = 0$ into five distinct regions.)

One might consider whether different polynomials could be used to distinguish these regions. This would provide different substitutions than those from Theorem 2.1 of [6]. Since the original substitutions are based on r and $\partial R/\partial s$, in the following section we examine cases in which s and $\partial R/\partial r$ can be used as separating polynomials instead.

4.2 Alternate substitutions

In this section we at a few alternatives to the substitutions based on r and a^* given by Weispfenning. Whether or not these substitutions may be applied depends on the coefficients of f, but is independent of g.

If $ac < 0$ we note that R is the product of two lines with opposite slopes (see the left plot from Figure 4.2). In this case $s = 0$ separates the $R < 0$ regions just as does $2as - rb = 0$, and $\partial R/\partial r = 4a(2cr - bs) = 0$ separates the $R < 0$ regions just as does $r = 0$.

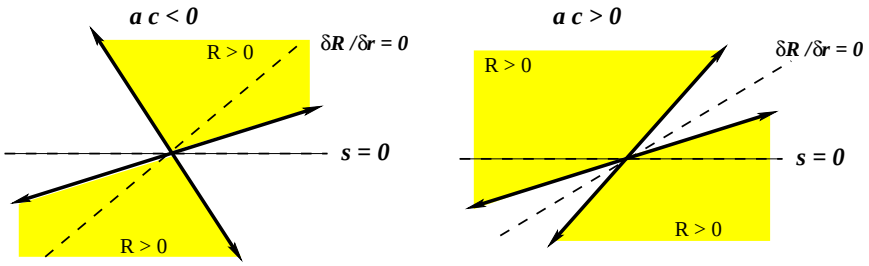

Figure 2: Plots of R, s and $\partial R/\partial r$ in (r, s)-space for $ac < 0$ and $ac > 0$.

If $ac > 0$, R is the product of two lines, both of which have positive slope if $ab > 0$, and negative slope if $ab < 0$ (see the right plot from Figure 4.2). In this case $s = 0$ separates the $R > 0$ regions just as does r, and $\partial R/\partial r = 4a(2cr - bs) = 0$ separates the $R < 0$ regions just as does $2as - rb = 0$.

Based on these observations, a variety of alternate substitutions can be formulated whose applicability is dependent on the signs of ac and R. Figure 4.2 lists some of them (note that c^* is used to refer to $2cr - bs$, so that $\partial R/\partial r = 4ac^*$). Each entry has been verified using quantifier elimination — Mathematica, Redlog and QEPCAD B all verify them almost instantly. At first glance, replacing a^* or r in the substitutions from Theorem 4 seems to require assumptions about the sign of R as well as ac. With one exception, however, a^* and r only appear in conjunction with the required sign condition on R, so that really only the sign of ac constrains our use of alternatives for a^* or r. The one exception is

$$
\begin{array}{ll}
\text{If } ac > 0 \wedge b^2 - 4ac \geq 0 \text{ then } & \left\{ \begin{array}{l}
R \leq 0 \Longrightarrow \operatorname{sgn}(r) = \operatorname{sgn}(abs) \\
R \geq 0 \Longrightarrow \operatorname{sgn}(a^*) = \operatorname{sgn}(-abc^*) \\
R = 0 \Longrightarrow \operatorname{sgn}(a^* r) = \operatorname{sgn}(-c^* s) \\
R \leq 0 \Longrightarrow (r = 0 \Longleftrightarrow s = 0) \\
R \geq 0 \Longrightarrow (a^* = 0 \Longleftrightarrow c^* = 0)
\end{array} \right. \\
\text{If } ac < 0 \wedge b^2 - 4ac \geq 0 \text{ then } & \left\{ \begin{array}{l}
R \leq 0 \Longrightarrow \operatorname{sgn}(r) = \operatorname{sgn}(-ac^*) \\
R \geq 0 \Longrightarrow \operatorname{sgn}(a^*) = \operatorname{sgn}(as) \\
R = 0 \Longrightarrow \operatorname{sgn}(a^* r) = \operatorname{sgn}(-c^* s) \\
R \leq 0 \Longrightarrow (r = 0 \Longleftrightarrow c^* = 0) \\
R \geq 0 \Longrightarrow (a^* = 0 \Longleftrightarrow s = 0)
\end{array} \right. \\
\text{If } ac \neq 0 \wedge b^2 - 4ac \geq 0 \text{ then } & \{R = 0 \Longrightarrow \operatorname{sgn}(a^* r) = \operatorname{sgn}(-c^* s)
\end{array}
$$

Figure 3: Alternate substitutions.

substitution (3) of Theorem 4, in which $pra^\delta \leq 0 \wedge a^* a^\delta$ is not explicitly guarded by any sign condition on R. The following theorem, whose simple proof we omit, states that $R = 0$ is actually implicit in this case, and therefore that we may freely replace a^* and r in the substitutions from Theorem 4 with the alternatives given in Figure 4.2 based solely on the sign of ac.

Theorem 11 *If $R \geq 0$ implies $X \iff a^* a^\delta < 0$ and $R \leq 0$ implies $Y \iff pra^\delta \leq 0$, then X can be used interchangeably with $a^* a^\delta < 0$ and Y can be used interchangeably with $pra^\delta \leq 0$ in substitution (3) of Theorem 4.*

In asking whether these substitutions are useful, it is helps to consider what happens generically. For example, when $f = ax^2 + bx + c$ and $g = ux^2 + vx + w$, we have $r = av - ub$, $s = aw - uc$, $a^* = 2a^2w - 2auc - bav + ub^2$ and $c^* = 2cav - cub - baw$. Clearly in this generic case, both s and c^* are "better" substitutions than a^*. In the non-generic case, when coefficients are constants or are algebraicly related, any one of these can be good or bad substitutions. What's interesting is that can generate each of them and choose the substitution that works best for each f, g combination in the context of the problem to be solved. Section 5.1 provides an interesting application of this approach.

5 Examples

This section steps through two example computations — the first involving a quadratic constraint, the second involving infinitesimals. The results of using the original substitutions are compared with using the improved substitution for infinitesimals from Section 3.2 and the alternate substitutions from Section 4.2. One difficulty in going through examples of virtual term substitution in detail is that the formulas are so large that they are hard to look at. We will endeavor to ameliorate this by showing only key parts of the substituted formulas, and by performing some reasonable simplifications before substituting. Also, we note that $R = a^n \mathrm{res}_x(f, g)$, so where R appears in formulas we will use $a^\delta \overline{R}$, where $\overline{R} = \mathrm{res}_x(f, g)$.

5.1 An example from epidemiology

Andreas Weber and his colleagues have been working on applying symbolic tools to investigations of epidemiological models, this example comes from his work. In considering the existence of an "endemic equilibrium" for the SEIT model [3], a system of ODEs used to model tuberculosis and other diseases, one arrives after straightforward calculations at the following formula:

$$\exists S \left[f(S) = 0 \ \wedge \ -S < 0 \wedge S - 1 < 0 \right]$$

where $f = \nu\beta_1(\beta_2 - \beta_1)S^2 + (d\beta_1 r_2 - d^2\beta_2 + d^2\beta_1 + \beta_1 r_1 r_2 - d\nu\beta_2 + \nu\beta_1 q r_2 - d\beta_2 r_2 + d\nu\beta_1 - \beta_1\nu\beta_2 + \beta_1 r_1 d)S + \beta_2 d(d+\nu+r_2)$, all parameters are positive, and $\beta_1 > \beta_2$. Note that the assumptions on the parameters imply that the coefficient of S^2 is negative and the coefficient of S^0 is positive. We will apply virtual term substitution to this problem. For the sake of brevity, however, we will not give the $a = 0$ substitution or the α_{+1} substitution, both of which produce obviously unsatisfiable subformulas. Thus, the quantified input formula is equivalent to:

$$a \neq 0 \wedge D \geq 0 \wedge g_1(\alpha_{-1}) < 0 \wedge g_2(\alpha_{-1}) < 0,$$

where $g_1 = -S$ and $g_2 = S - 1$. Since the quadratic and constant coefficients have opposite signs, $a \neq 0 \wedge D \geq 0$ is always true, so we will proceed with $g_1(\alpha_{-1}) < 0 \wedge g_2(\alpha_{-1}) < 0$. Since $p = -1$, g_1 and g_2 have degree 1, and a is always negative we will reduce $a^*a^\delta < 0 \wedge a^\delta\overline{R} > 0 \vee pra^\delta \leq 0 \wedge (a^*a^\delta < 0 \vee a^\delta\overline{R} < 0)$ to

$$-a^* < 0 \wedge -\overline{R} > 0 \vee r \leq 0 \wedge (-a^* < 0 \vee -\overline{R} < 0)$$

Following Weispfenning's original substitutions restated in Theorem 4, we get:

$$\left[\begin{array}{c} -(d\beta_1 r_2 - \beta_2 d^2 + d^2\beta_1 + \beta_1 r_1 r_2 - \nu\beta_2 d + \nu\beta_1 q r_2 - \beta_2 d r_2 + d\nu\beta_1 - \beta_1\nu\beta_2 \\ +\beta_1 r_1 d) < 0 \wedge -(d\beta_2(d+\nu+r_2)) > 0 \vee -1 \leq 0 \wedge [-(d\beta_1 r_2 - \beta_2 d^2 \\ +d^2\beta_1 + \beta_1 r_1 r_2 - \nu\beta_2 d + \nu\beta_1 q r_2 - \beta_2 d r_2 + d\nu\beta_1 - \beta_1\nu\beta_2 + \beta_1 r_1 d) < 0 \\ \vee -(d\beta_2(d+\nu+r_2)) < 0] \end{array}\right]$$
$$\wedge$$
$$\left[\begin{array}{c} -(2\nu\beta_1^2 - \beta_1\nu\beta_2 - d\beta_1 r_2 + \beta_2 d^2 - d^2\beta_1 - \beta_1 r_1 r_2 + \nu\beta_2 d - \nu\beta_1 q r_2 + \beta_2 d r_2 \\ -d\nu\beta_1 - \beta_1 r_1 d) < 0 \wedge -(\beta_1(-\beta_1\nu + r_2 d + d^2 + r_1 r_2 + \nu q r_2 + d\nu \\ +dr_1)) > 0 \vee 1 \leq 0 \wedge (-(2\nu\beta_1^2 - \beta_1\nu\beta_2 - d\beta_1 r_2 + \beta_2 d^2 - d^2\beta_1 - \\ \beta_1 r_1 r_2 + \nu\beta_2 d - \nu\beta_1 q r_2 + \beta_2 d r_2 - d\nu\beta_1 - \beta_1 r_1 d) < 0 \vee -(\beta_1(-\beta_1\nu \\ +r_2 d + d^2 + r_1 r_2 + \nu q r_2 + d\nu + dr_1)) < 0) \end{array}\right].$$

Noting that $d\beta_2(d+\nu+r_2)$ is always positive and simplifying away inequalities involving only constants, we get:

$$\begin{array}{c} 2\nu\beta_1^2 - \beta_1\nu\beta_2 - d\beta_1 r_2 + \beta_2 d^2 - d^2\beta_1 - \beta_1 r_1 r_2 + \nu\beta_2 d - \nu\beta_1 q r_2 + \beta_2 d r_2 \\ -d\nu\beta_1 - \beta_1 r_1 d > 0 \wedge -\beta_1\nu + r_2 d + d^2 + r_1 r_2 + \nu q r_2 + d\nu + dr_1 < 0 \end{array} \quad (2)$$

However, we are in the $ac < 0$ case, so we may replace a^* with as according to Figure 4.2. Since $s_1 = 0$ and $s_2 = -1$ and a is known to be negative, this alternate substitution is well worth taking. With it we get:

$$\left[\begin{array}{c} -(-0) < 0 \wedge -(d\beta_2(d+\nu+r_2)) > 0 \vee \\ -1 \leq 0 \wedge [-(0) < 0 \vee -(d\beta_2(d+\nu+r_2)) < 0] \end{array}\right]$$
$$\wedge$$
$$\left[\begin{array}{c} -(-(-1)) < 0 \wedge -(\beta_1(-\beta_1\nu + r_2 d + d^2 + r_1 r_2 + \nu q r_2 + d\nu + dr_1)) > 0 \\ \vee 1 \leq 0 \wedge \\ \left[-(-(-1)) < 0 \vee -(\beta_1(-\beta_1\nu + r_2 d + d^2 + r_1 r_2 + \nu q r_2 + d\nu + dr_1)) < 0\right] \end{array}\right]$$

After making the obvious simplifications we get:

$$-\beta_1\nu + r_2 d + d^2 + r_1 r_2 + \nu q r_2 + d\nu + d r_1 < 0 \tag{3}$$

The final simplification of (2) to (3) is not trivial. The assumptions on the parameters do not imply the positivity of the extraneous polynomial. It is only those assumptions in conjunction with $-\beta_1\nu+r_2d+d^2+r_1r_2+\nu qr_2+d\nu+dr_1 < 0$ that imply it. This is a simplification that Redlog's simplifier, for example, is not able to make.

5.2 Substituting infinitesimals

Let $f = ax^2+bx+1$ and $g = ux^2+vx-1$. We consider the formula $\exists x[f < 0 \wedge g < 0]$ under the assumption $a, u > 0$. First we will follow the original method, then we will apply the improved substitutions for infinitesimals as well as alternate substitutions from the previous section. Rather than write out the entire formula here, we simply write out the set of polynomials appearing in the formula, and show one representative subformula, the substitution for $g(\alpha_{-1}+\epsilon) < 0$. In addition to the coefficients of f and g, the following polynomials appear in the formula produced by Theorem 7:

$$\begin{array}{l} D_f = b^2 - 4a,\ D_g = v^2 + 4u,\ r = av - ub,\ s = -a - u \\ \overline{R} = u^2 + 2au + a^2 - vub + bav + av^2 - ub^2 \\ a^* = -2a^2 - 2au - bav + ub^2,\ a_g^* = 2u^2 + 2au - vub + av^2 \\ \overline{R}_{g_x} = 4u^2 - 2vub + av^2,\ \overline{R}_{f_x} = -4a^2 - 2bav + ub^2 \\ c^* = 2av - ub + ab,\ c_g^* = av - 2ub - vu \end{array} \tag{4}$$

The original substitution for $g(\alpha_{-1}+\epsilon) < 0$ is:

$$\overbrace{\left(\begin{array}{c} a^* < 0 \wedge \overline{R} > 0 \\ \vee - r \leq 0 \wedge \\ (a^* < 0 \vee \overline{R} < 0)) \end{array}\right)}^{g(\alpha_{-1})<0} \vee \underbrace{\left(\begin{array}{c} -ra^* \leq 0 \\ \wedge \\ \overline{R} = 0 \end{array}\right)}_{g(\alpha_{-1})=0} \wedge \left(\begin{array}{c} \overbrace{\left(\begin{array}{c} 2ra < 0 \wedge a\overline{R}_{g_x} > 0 \\ \vee - 2ua \leq 0 \wedge \\ (2ra < 0 \vee a\overline{R}_{g_x} < 0)) \end{array}\right)}^{g_x(\alpha_{-1})<0} \\ \vee \\ \underbrace{-4ur \leq 0 \wedge a\overline{R}_{g_x} = 0 \wedge 2u < 0}_{g_x(\alpha_{-1})=0 \wedge 2u<0} \end{array}\right)$$

Although the other substitutions are not shown, it should be clear that the entire formula is constructed out of the polynomials in (4) and a, b, u, v.

The substitution given in Section 3.2 gives the following for $g(\alpha_{-1}+\epsilon) < 0$:

$$\begin{array}{c} (a^* < 0 \wedge \overline{R} > 0 \vee -r \leq 0 \wedge (a^* < 0 \vee \overline{R} < 0)) \\ \vee \\ \overline{R} = 0 \wedge (r = 0 \wedge -u < 0 \vee -a^* r \leq 0 \wedge r a_g^* < 0 \vee -a^* r < 0 \wedge a_g^* = 0 \wedge u < 0) \end{array}$$

Although the other substitutions are not shown, it should be clear that the entire formula is constructed out of a, b, u, v and the polynomials in (4) minus $\overline{R}_{g_x}$ and $\overline{R}_{f_x}$.

Clearly f falls in the $ac > 0$ case and g falls in the $ac < 0$ case discussed in Section 4.2. Thus, we may choose alternate substitutions given there. This leads to a substitution for $g(\alpha_{-1} + \epsilon) < 0$ of:

$$\begin{gathered}(-abc^* < 0 \wedge R > 0 \vee -abs \leq 0 \wedge (-abc^* < 0 \vee R < 0)) \\ \vee \\ R = 0 \wedge (s = 0 \wedge -u < 0 \vee sc^* \leq 0 \wedge sc_g^* < 0 \vee sc^* < 0 \wedge us = 0 \wedge u < 0)\end{gathered}$$

Whether or not this is "better" than the previous formula depends on what subsequent computation is desired. It is interesting, however, that it is trivial to deduce that the input assumptions $a, u > 0$ implies $s > 0$, which then considerably simplifies the formula. It is also interesting that after removing all polynomials that, by inspection, never vanish given $a, u > 0$, this final version contains only 2 polynomials that are not linear — $\overline{R}$ and D_f. In contrast, the original contains 4 non-linear polynomials. The potential advantage to alternate substitutions is that a program may quickly examine the alternatives and decide whether, as in this case, one offers advantages over the other.

6 Improved bound for virtual term substitution

The fact that $\text{res}_x(f, g) = (a^{*2} - b^{*2}D)/(4a^n)$ allows one to tighten the most general degree bound given in Corollary 2.2 of [6]. Suppose that M is the maximum total degree of any polynomial in the input, and that d is the greatest degree in x of any polynomial in the input.

Theorem 12 *The highest degree of any irreducible factor of a polynomial appearing in the formula produced by Theorem 2.1 of [6] is* $(d+2)M - 2d$.

Proof. Note that the total degree of the coefficient of x^m is at most $M-m$. The candidates for the highest degree factors are $b^2 - 4ac$, b^*, a^* and $a^{*2} - b^{*2}c$. The degree of $b^2 - 4ac$ is clearly bounded by $2M - 2$. $a^{*2} - b^{*2}c$ is the determinant of the Sylvester matrix for f and g, and r and s are given by minors of the Sylvester matrix. We will show explicitly that the largest irreducible factor of $a^{*2} - b^{*2}c$ has total degree at most $(d+2)M - 2d$. A similar approach shows that r and s have total degrees at most $dM - 2d + 1$ and $dM - 2d + 2$, respectively. Thus, $a^* = 2as - br$ has total degree at most $\max((M-1) + dM - 2d + 1, (M - 2) + dM - 2d + 2) = (d+1)M - 2d$.

$\text{res}_x(f, g) = (a^{*2} - b^{*2}D)/(4a^n)$, the degree of the largest irreducible factor of $a^{*2} - b^{*2}D$ is bounded from above by the degree of $\text{res}_x(g, f)$. Assume g has the

maximal x-degree d. The rows of the Sylvester matrix for g and f correspond to $xg, g, x^{n-2}f, x^{n-1}f, \ldots, x^0 f$. The determinant is the sum of all products of one element from each row and each column. Consider choosing elements to form such a product. Suppose that i and j, $i < j$, are the indices of the entries chosen from the first two rows. From columns $1, \ldots, i-1$ we must choose the a entry in order to get a non-zero product (a has degree at most $M-2$). From columns $j+1, \ldots, d+2$ we must choose the c entry to get a non-zero product (degree M). The submatrix remaining after all these choices is tridiagonal with a's below, b's on and c's above the diagonal. Any entry chosen above the diagonal must be matched with an entry below the diagonal, so the average total degree is $(M-1)$. The product of the two entries from the first two rows has degree $2M - 2d + i + j - 3$. Thus, any term in the determinant has degree at most

$$(i-1)(M-2)+(j-i-1)(M-1)+(d+2-j)M+(2M-2d+i+j-3) = (d+2)M-2d.$$

□

Corollary 2.2 of [6] gives a bound of $(2d+2)M-2d$ on any polynomial appearing in the formula. The new bound is approximately a factor of two improvement, although of course it is a bound on the size of irreducible factors. The bound from Corollary 2.2 also assumes that the total degree of f is not more than the maximum total degree of $p(F)$. The above analysis makes no such assumption.

7 Conclusion

This paper provides an analysis of the polynomials appearing in Weispfenning's method of quantifier elimination by virtual term substitution. Based on this analysis, and simpler substitution is given for the evaluation of a formula at $x = \alpha + \epsilon$, where α is the root of a quadratic polynomial and ϵ is a positive infinitesimal. The paper proceeds with a new view on *why* certain polynomials appear in substitutions and, based on this, proposes alternate substitutions. These alternatives are not always applicable but, when they are, they allow for an implementation of virtual term substitution that can choose amongst alternatives in order to produce simpler formulas. Both of these improvements are aimed at helping reduce the complexity of the result of quantifier elimination by virtual term substitution, which is the method's biggest problem.

8 Acknowledgements

This work was supported by NSF grant number CCR-0306440.

References

[1] Buchberger, B., Collins, G. E., Loos, R., and Albrecht, R., Eds. *Computer algebra: symbolic and algebraic computation (2nd ed.)*. Springer-Verlag New York, Inc., New York, NY, USA, 1983.

[2] Dolzmann, A., and Sturm, T. Redlog: Computer algebra meets computer logic. *ACM SIGSAM Bulletin 31*, 2 (June 1997), 2–9.

[3] van den Driessche, P., and Watmough, J. Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission. *Mathematical Biosciences 180* (2002), 29–48.

[4] Weispfenning, V. The complexity of linear problems in fields. *Journal of Symbolic Computation 5* (1988), 3–27.

[5] Weispfenning, V. Quantifier elimination for real algebra — the cubic case. In *Proc. International Symposium on Symbolic and Algebraic Computation* (1994), pp. 258–263.

[6] Weispfenning, V. Quantifier elimination for real algebra — the quadratic case and beyond. *AAECC 8* (1997), 85–101.

[7] Weispfenning, V. Simulation and optimization by quantifier elimination. *J. Symb. Comput. 24*, 2 (1997), 189–208.